Claims

1. A method for transmitting first information (Goods) from a user (Customer) of a telecommunication network to a first provider (Seller)
and second information (X.509 Identity Certificate) from said user (Customer) to a second provider (Bank),
wherein the first information (Goods) can be encrypted in accordance with specifications of the first provider (Seller)
and
wherein the second information contains a single- or multi-part component (Payment Info) which is encrypted in accordance with specifications of the second provider (Bank)
and wherein the information is sent in a common information unit.

2. A method for transmitting first information (Goods) from a user (Customer) of a telecommunication network to a first provider (Seller)
and second information (X.509 Attribute Certificate) from said user (Customer) to a second provider (Bank),
wherein the first information (Goods) can be encrypted in accordance with specifications of the first provider (Seller)
and
wherein the second information contains a single- or multi-part component (Payment Info) which is encrypted in accordance with specifications of the second provider (Bank)
and wherein the second information is stored by the first or second seller in a data memory which can be accessed by the first and second seller.

3. The method as claimed in claim 1 or 2,
characterized in that
a private extension of a certificate conforming to the X.509 standard is used for storing the second information.

4. The method as claimed in one of the preceding claims,
characterized in that
it is used for a payment transaction and the transmitted first and/or second information relates to the payment transaction.

5. The method as claimed in claim 4,
characterized in that
a unique transaction number (TAN) is assigned to the payment transaction by the second provider or by the user.

6. The method as claimed in claim 4,
characterized in that
an identity certificate extension is used.

7. The method as claimed in claim 4,
characterized in that
an attribute certificate extension is used.

8. The method as claimed in claim 7,
characterized in that
an attribute certificate can be used precisely once.

9. The method as claimed in one of the preceding claims,
characterized in that
a suitable storage medium, in particular a smart card, smart dongle or a storage medium that can be read contactlessly, is used for storing the certificate.

10. The method as claimed in one of the preceding claims, characterized in that
the certificate is stored on the storage medium, protected by a password.